NSE4_FGT-7.2 Q&As

Fortinet NSE 4 - FortiOS 7.2

QUESTION 1

An administrator has configured two-factor authentication to strengthen SSL VPN access. Which additional best practice can an administrator implement?

A. Configure Source IP Pools.

B. Configure split tunneling in tunnel mode.

C. Configure different SSL VPN realms.

D. Configure host check .

Correct Answer: D

QUESTION 2

What are two features of collector agent advanced mode? (Choose two.)

A. In advanced mode, FortiGate can be configured as an LDAP client and group filters can be configured on FortiGate.

B. In advanced mode, security profiles can be applied only to user groups, not individual users.

C. Advanced mode uses the Windows convention--NetBios: Domain\Username.

D. Advanced mode supports nested or inherited groups.

Correct Answer: AD

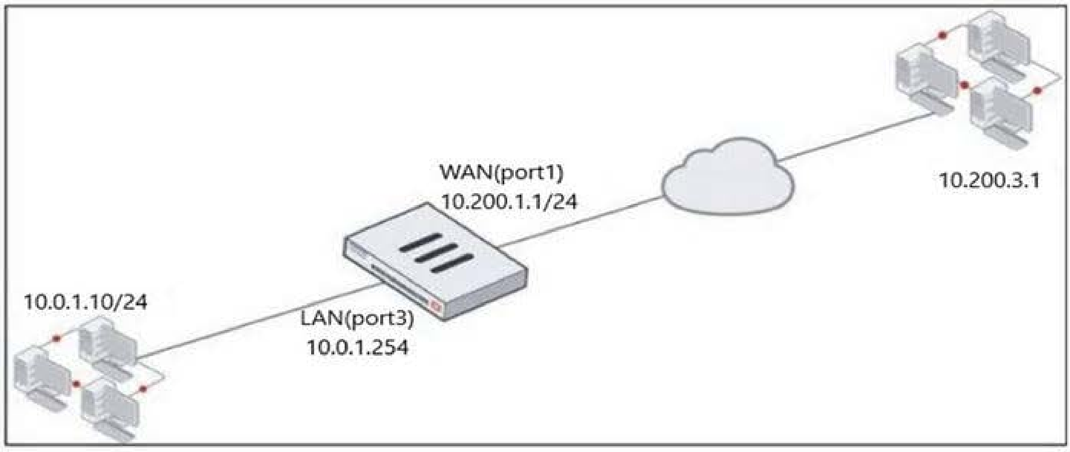
In advanced mode, FortiGate can be configured as an LDAP client and group filters can be configured on FortiGate. This is true because advanced mode allows FortiGate to query the LDAP server directly for user information and group membership, without relying on the collector agent. This enables FortiGate to apply security policies based on LDAP group filters, which can be configured on FortiGate1 Advanced mode supports nested or inherited groups. This is true because advanced mode can handle complex group structures, such as nested groups or inherited groups, where a user belongs to a group that is a member of another group. This allows FortiGate to apply security policies based on the effective group membership of a user, not just the direct group membership1

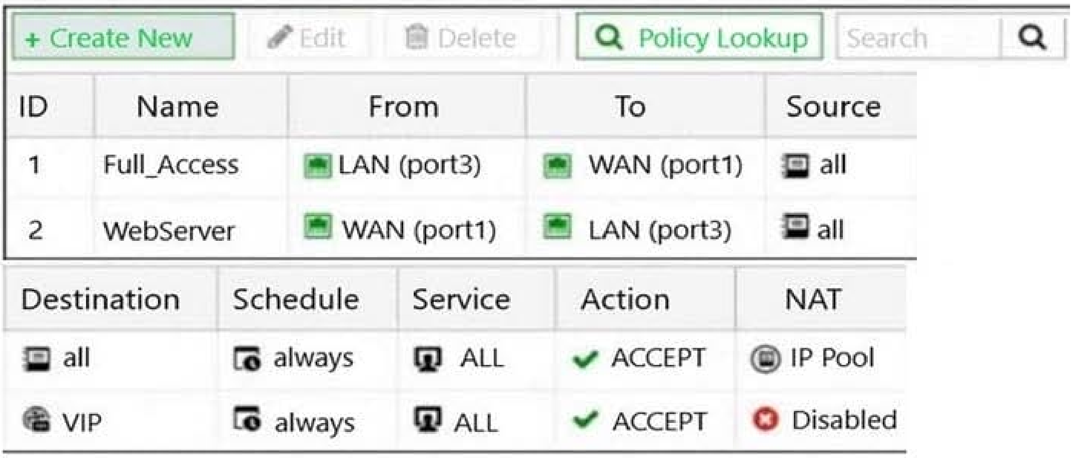
FortiGate Infrastructure 7.2 Study Guide (p.146): "Also, advanced mode supports nested or inherited groups; that is, users can be members of subgroups that belong to monitored parent groups." "In advanced mode, you can configure FortiGate as an LDAP client and configure the group filters on FortiGate. You can also configure group filters on the collector agent."

QUESTION 3

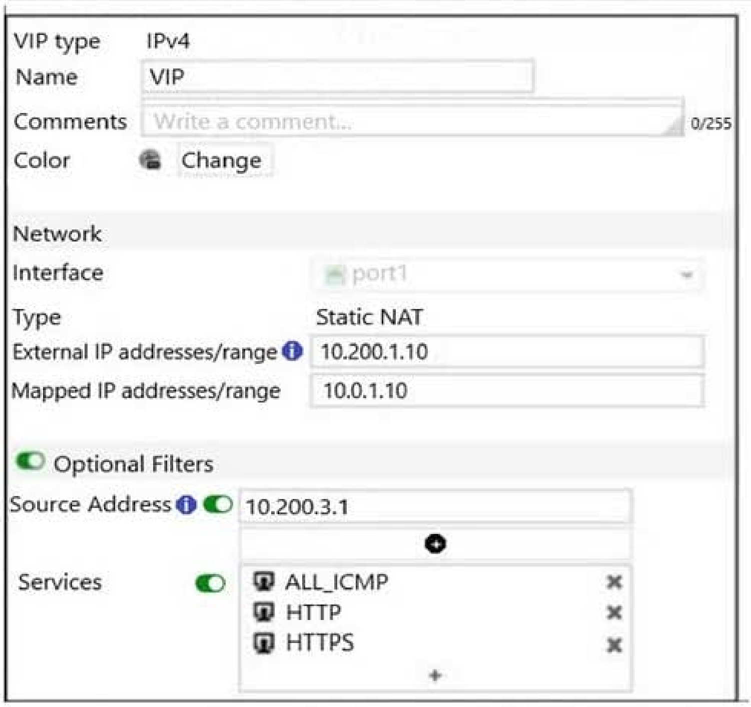
Refer to the exhibits.

The exhibits contain a network diagram, virtual IP, IP pool, and firewall policies configuration.





ID	Name	From	To	Source	Destination	Schedule	Service	Action	NAT
1	Full_Access	LAN (port3)	WAN (port1)	all	all	always	ALL	✓ ACCEPT	IP Pool
2	WebServer	WAN (port1)	LAN (port3)	all	VIP	always	ALL	✓ ACCEPT	Disabled



VIP type IPv4

Name VIP

Comments Write a comment... 0/255

Color Change

Network

Interface port1

Type Static NAT

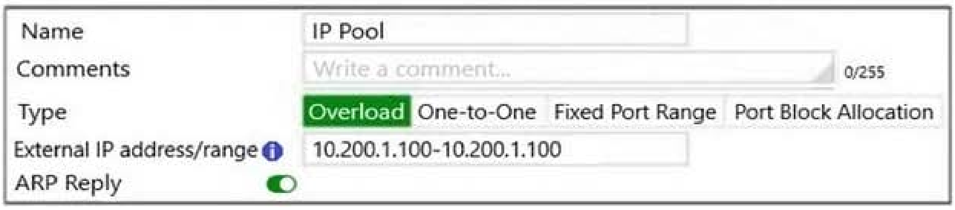
External IP addresses/range 10.200.1.10

Mapped IP addresses/range 10.0.1.10

Optional Filters

Source Address 10.200.3.1

Services ALL_ICMP HTTP HTTPS



Name IP Pool

Comments Write a comment... 0/255

Type [✓ Overload] One-to-One Fixed Port Range Port Block Allocation

External IP address/range 10.200.1.100-10.200.1.100

ARP Reply

The WAN (port1) interface has the IP address 10.200.1.1/24.

The LAN (port3) interface has the IP address 10.0.1.254/24.

The first firewall policy has NAT enabled using IP Pool.

The second firewall policy is configured with a VIP as the destination address.

Which IP address will be used to source NAT the internet traffic coming from a workstation with the IP address 10.0.1.10?

A. 10.200.1.100

B. 10.200.1.10

C. 10.200.1.1

D. 10.200.3.1

Correct Answer: A

Policy 1 is applied on outbound (LAN-WAN) and policy 2 is applied on inbound (WAN-LAN). question is asking SNAT for outbound traffic so policy 1 will take place and NAT overload is in effect.

QUESTION 4

By default, FortiGate is configured to use HTTPS when performing live web filtering with FortiGuard servers.

Which CLI command will cause FortiGate to use an unreliable protocol to communicate with FortiGuard servers for live web filtering?

A. set fortiguard-anycast disable

B. set webfilter-force-off disable

C. set webfilter-cache disable

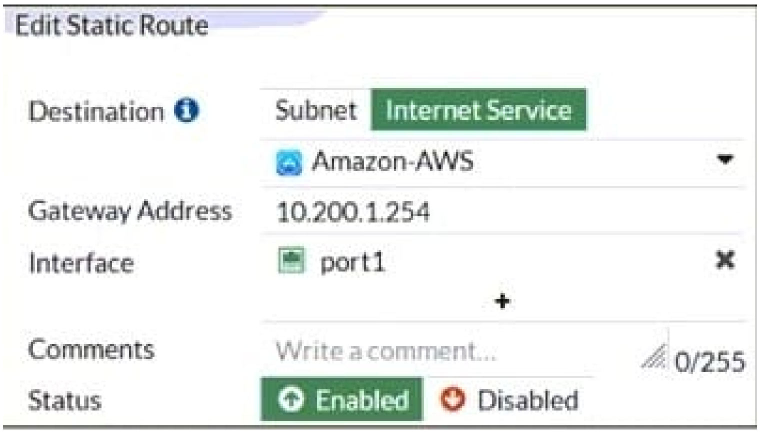
D. set protocol tcp

Correct Answer: A

Reference: https://kb.fortinet.com/kb/documentLink.do?externalID=FD48294

QUESTION 5

Refer to the exhibit, which contains a static route configuration. An administrator created a static route for Amazon Web Services.



Edit Static Route

Destination	Subnet [✓ Internet Service] Amazon-AWS
Gateway Address	10.200.1.254
Interface	port1
Comments	Write a comment... 0/255
Status	[✓ Enabled] Disabled

Which CLI command must the administrator use to view the route?

A. get router info routing-table database

B. diagnose firewall route list

C. get internet-service route list

D. get router info routing-table all

Correct Answer: B

ISDB static route will not create entry directly in routing-table. Reference: https://community.fortinet.com/t5/FortiGate/Technical-Tip-Creating-a-static-route-for- Predefined-Internet/ta-p/198756 and here https://community.fortinet.com/t5/FortiGate/Technical-Tip-Verify-the-matching- policy-route/ta-p/190640

FortiGate Infrastructure 7.2 Study Guide (p.16 and p.59): "Even though they are configured as static routes, ISDB routes are actually policy routes and take precedence over any other routes in the routing table. As such, ISDB routes are added to the policy routing table." "FortiOS maintains a policy route table that you can view by running the diagnose firewall proute list command."

NSE4_FGT-7.2 PDF Dumps NSE4_FGT-7.2 Practice Test NSE4_FGT-7.2 Exam Questions